09 FEB 1989

OCA - 0348-89

Mr. Howard Rhile
Associate Director
Information Management
and Technology Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Rhile:

The Director has asked me to respond to your letter of January 27, 1989 requesting completion of a questionnaire intended to determine federal agencies compliance with Section 6(b) of the Computer Security Act of 1987, Public Law 100-235, January 8, 1988.

After a thorough review of the various computer systems at the Central Intelligence Agency, we have determined that none of our systems are subject to the reporting requirements of the Act. This decision was based on 44 U.S.C. Section 3502(2).

Sincerely,

STAT

[redacted]

// John L. Helgerson
Director of Congressional Affairs

OCA/SA/EC: SGB (7 Feb 89)

DISTRIBUTION:
Orig - Addressee
1 - D/OCA
1 - OCA Record
1 - EC Chrono
1 - D/OS
1 - IG
1 - D/OIT/DA
1 - ER
1 - DDA
1 - OGC
1 - Compt

GAO

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

ER 89-0393

JAN 27 1989

WILLIAM H. WEBSTER
CENTRAL INTELLIGENCE AGENCY
WASHINGTON, DC 20505

According to your agency's response to our previous Computer Security Act of 1987 Questionnaires, you had not identified any federal computer systems that contain sensitive information. Even though you responded in that manner, we have enclosed a questionnaire addressing section 6(b) of the Computer Security Act of 1987. Section 6(b) is aimed at the establishment of computer security plans for the security and privacy of federal computer systems that contain sensitive information. Please answer and return the enclosed questionnaire, whether or not you have identified any federal computer systems containing sensitive information since responding to our previous questionnaires.

Thank you for your cooperation.

Sincerely yours,

Howard Rhile

Howard Rhile
Associate Director

GAO

United States
General Accounting Office
Washington, D.C. 20548

Information Management and
Technology Division

JAN 27 1988

WILLIAM H. WEBSTER
CENTRAL INTELLIGENCE AGENCY
WASHINGTON, DC 20505

The United States General Accounting Office (GAO), part of the legislative branch, assists the Congress in oversight of the executive branch of the federal government. GAO's major responsibilities include evaluating and auditing programs, activities, and financial operations of federal departments and agencies and making recommendations for improving government operations. The Chairmen of the House Committees on Government Operations and Science, Space, and Technology, respectively, asked us to ascertain the extent to which federal agencies are complying with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. (Job code 510306.)

To obtain information on the status of compliance, we are sending three questionnaires to federal agencies. The first and second, which you have already received, addressed section 6(a) and section 5 of the act. Section 6(a) is directed at the identification of federal computer systems that contain sensitive information. Section 5 is aimed at the establishment of computer security training for employees involved with the management, use, or operation of such systems.

The final questionnaire, which is enclosed, addresses section 6(b) of the act. Section 6(b) requires that each federal agency, within one year of the act's enactment, establish a plan for the security and privacy of federal computer systems that contain sensitive information that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system.

The enclosed questionnaire is being sent to you as the senior information resource management (or comparable) official in your agency. Please complete and return the questionnaire in the enclosed envelope within 10 days of receipt. Please be sure to include in your response information for all offices, bureaus, services, etc. within your agency. If you have any questions, please call David Gill or Deborah Davis at (202) 275-9675.

Thank you for your cooperation.

Sincerely yours,

Howard Rhile

Howard Rhile
Associate Director

U.S. General Accounting Office

COMPUTER SECURITY ACT OF 1987 QUESTIONNAIRE

The U.S. General Accounting Office (GAO) has been asked by the Chairmen of the House Committees on Government Operations and Science, Space, and Technology to review federal agencies' compliance with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. In response, we are sending questionnaires to federal agencies in order to ascertain the extent to which they are in compliance.

The previous questionnaires, which you have already received, addressed section 6(a) and section 5 of the act. They were used to obtain information on the status of federal agencies' identification of federal computer systems that contain sensitive information and the establishment of computer security training.

The final questionnaire, which is enclosed, addresses section 6(b) of the act which is aimed at the establishment of computer security plans for the security and privacy of each federal computer system containing sensitive information.

Please return the completed questionnaire in the enclosed self-addressed envelope within 10 days of receiving it. If the return envelope has been lost, please send the completed questionnaire to Loraine Przybylski, U.S. General Accounting Office, Room 6075, 441 G St., N.W., Washington, D.C. 20548. If you have any questions, please call David Gill or Deborah Davis at (202) 275-9675. Thank you for your help.

---

1. Agency name _____

2. Agency address _____

3. Responsible official to contact for more information, if needed.

   Name _____
   Department/Office _____
   Address _____
   _____
   Telephone number _____

4. Does your agency have federal computer systems, either currently operational or under development, that contain sensitive information and are within or under the supervision of your agency? Consider systems that are operated by your agency, a contractor of your agency, or other organizations that process information on your behalf. Exclude systems you operate for another agency.

(CHECK ONE)

____ YES
____ NO (GO TO QUESTION 14)

5. Did your agency submit security plans for all of your federal Computer systems containing sensitive information, including systems operated by other federal agencies, contractors, grantees, state or local governments, or others that process information on your agency's behalf to accomplish a federal function, to the National Institute of Standards and Technology (NIST) by January 8, 1989, as required by PL100-235?

____ YES
____ NO

If no, please list the system(s) for which plans are still due, and the date each plan will be submitted to NIST.

SYSTEM	DATE PLAN WILL BE SUBMITTED
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

6. By operator of the system, indicate the number of security plans submitted to NIST, and the number of systems covered by those plans.

(OPERATOR)	Plans	Systems
Your agency	_____	_____
Another federal agency	_____	_____
Contractor	_____	_____
State or local governments	_____	_____
Other (specify)_____	_____	_____
Total	_____	_____

7. The act requires that your security plans for systems containing sensitive information be "commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system." For each of your systems containing sensitive information, how has your agency determined the risks and developed protection requirements? (Please explain if your agency determined the risks to each of your systems in different ways.)

(CHECK ONE)

____ used formal risk analysis prepared to comply specifically with OMB Circular A-123

____ used formal risk analysis prepared to comply specifically with OMB Circular A-130

____ used same formal risk analysis to comply with OMB Circular A-123, OMB Circular A-130, and the Computer Security Act of 1987

____ performed formal risk analysis independent of the requirements of OMB Circular A-123 and OMB Circular A-130

____ other method (please explain) _____

_____

_____

_____

8. Do your security plans include specific provisions to identify and restrict threats such as viruses or other malicious code?

____ YES, for all plans

____ YES, for some plans (please indicate which plans)_____

_____

____ NO

9. Are your computer security plans consistent with your agency's

(CHECK ALL THAT APPLY)
____ information security procedures and directives
____ information resource management procedures and directives
____ information resource management plan
____ 5-year ADP plan required by 44 U.S.C. 3505

If your computer security plans are not consistent with any of the guidance listed above or your have not developed any of the above guidance, please explain.

_____
_____
_____
_____
_____
_____
_____
_____

10. Were the following staff part of the preparation and review process for your computer security plans?

(CHECK ALL THAT APPLY)
____ senior information resource management official
____ senior managers
____ functional or program managers
____ security managers
____ auditors
____ end user personnel
____ system development personnel
____ system maintenance personnel
____ other (specify) _____

11. Provide the title of the highest level of staff reviewing your security plans within your agency.

_____

12. The Office of Management and Budget (OMB) issued OMB Bulletin 88-16 as guidance for preparing the required security plans. OMB also sent a September 6, 1988, memorandum to senior information resource management officials containing answers to commonly asked questions about implementing the act. How satisfied was your agency with this guidance?

(CHECK ONE)
____ very satisfied
____ satisfied
____ neither satisfied nor dissatisfied
____ dissatisfied
____ very dissatisfied
____ did not use OMB's guidance

13. Was the OMB guidance helpful in preparing your security plans?

(CHECK ONE)
____ (YES)
____ (NO)
____ (NO OPINION)

Please provide below any comments on OMB's guidance.

14. If you have any comments about any questions on this form, or if you have any questions you believe we should have asked but did not, please write them below.

Thank you for your cooperation.